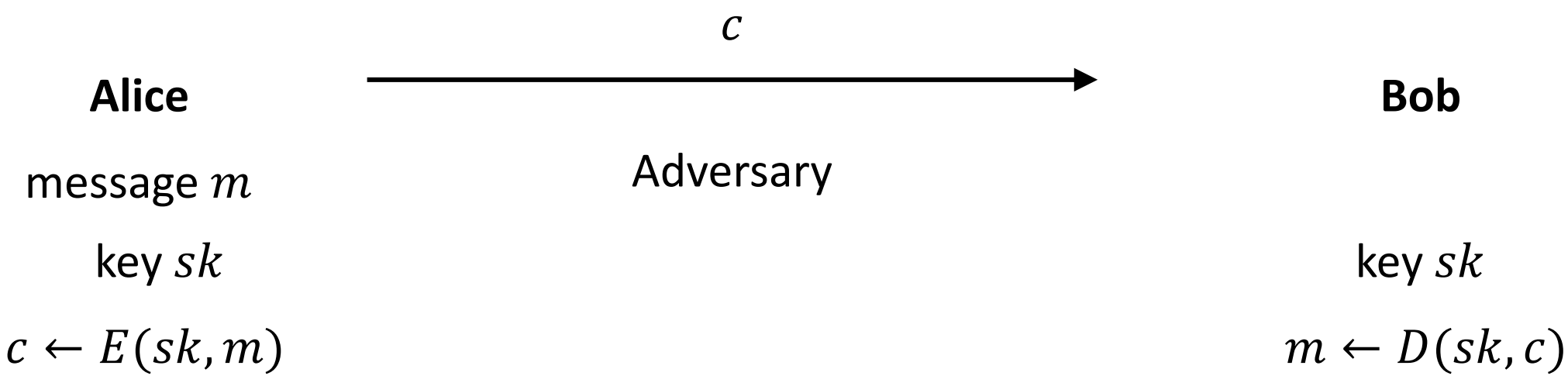
Foundations of Cryptography

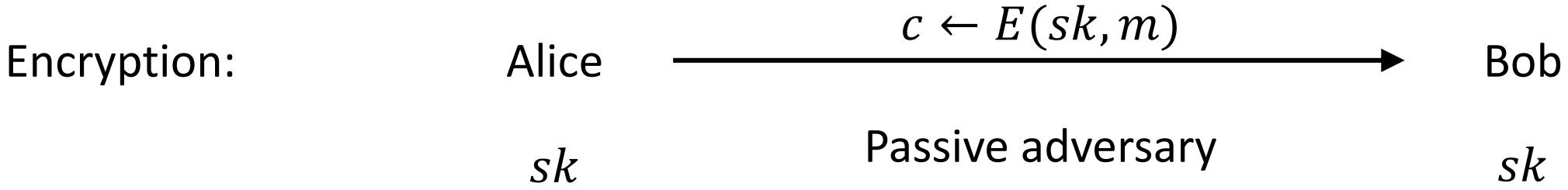
Week 6

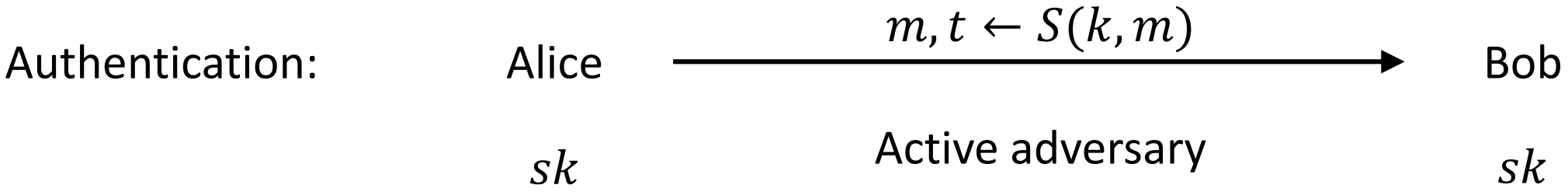
Omer Paneth

Symmetric Encryption



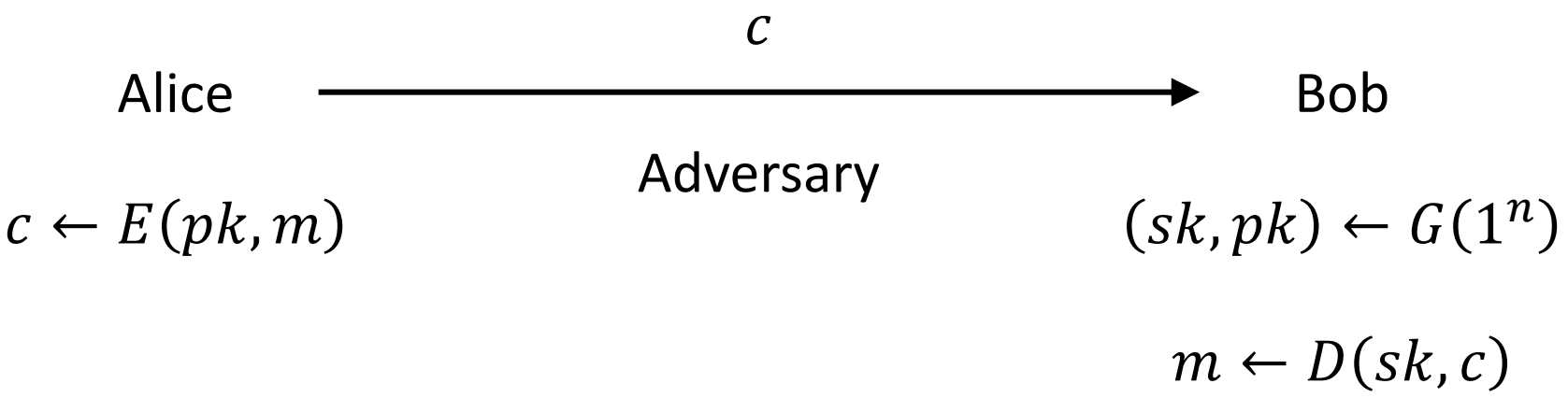
Symmetric Crypto





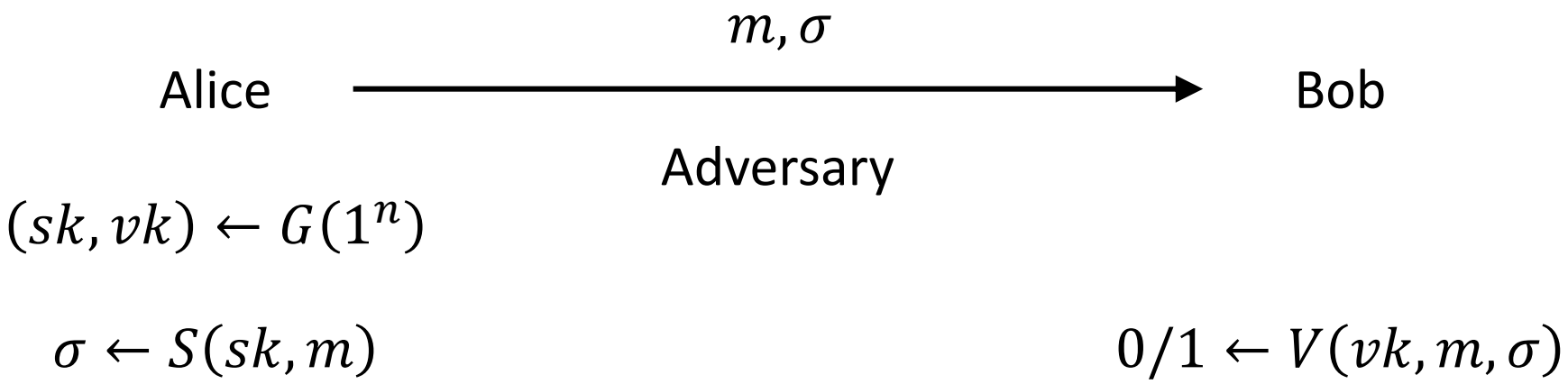
Public-Key Encryption (PKE)

Bob's public encryption key: pk



Digital Signature

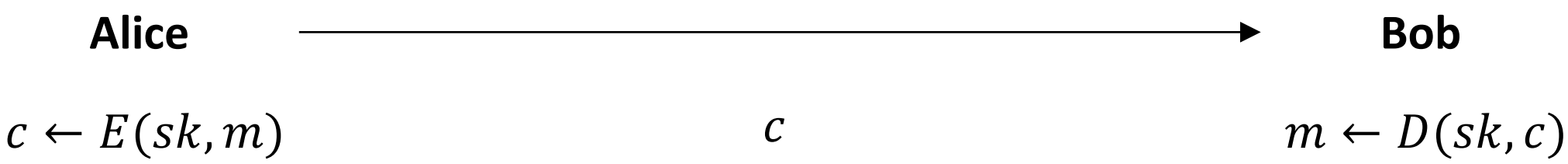
Alice's public verification key: vk



Symmetric Encryption - Definition

Syntax: an encryption scheme consists of three PPT algorithms (G, E, D):

- Key generation algorithm $G(1^n) \rightarrow sk \in \{0,1\}^n$
- Encryption algorithm $E(sk, m \in \{0,1\}^*) \rightarrow c$
- Deterministic decryption algorithm $D(sk, c) \rightarrow m$



Symmetric Encryption - Definition

Correctness: for any $n \in \mathbb{N}$ and message $m \in \{0,1\}^*$:

$$\Pr_{sk \leftarrow G(1^n)}\left[D\left(sk, E(sk, m)\right) = m\right] = 1$$

Security: ?

Computational Security

Definition: A cipher (G, E, D) is computationally secure for messages of length $\ell = \ell(n)$ if for every poly-size adversary $A = \{A_n\}$ there exists a negligible function ϵ such that for any $n \in \mathbb{N}$ and messages $m_0, m_1 \in \{0,1\}^\ell$:

$$\Pr_{\substack{sk \leftarrow G(1^n) \\ b \leftarrow \{0,1\}}}\left[A_n\left(E(sk, m_b)\right) = b\right] \leq \frac{1}{2} + \epsilon(n)$$

Equivalently: (G, E, D) is computationally secure if:

$$\{E(sk, m_0)\}_{\substack{n \in \mathbb{N} \\ m_1, m_2 \in \{0,1\}^\ell}} \approx_c \{E(sk, m_1)\}_{\substack{n \in \mathbb{N} \\ m_1, m_2 \in \{0,1\}^\ell}}$$

where $sk \leftarrow G(1^n)$.

Symmetric Encryption

Theorem: There exists a computationally secure cipher for messages of length n.

If fact, the cipher is perfectly secure ($\epsilon = 0$ against unbounded A).

Proof:

- $G(1^n)$ sample $sk \leftarrow \{0,1\}^n$ and output sk
- $E(sk, m \in \{0,1\}^n)$ outputs $ct = sk \oplus m$
- $D(sk, ct)$ outputs $m = sk \oplus ct$

One Time Pad (OTP)

Correctness:

$$D\big(sk, E(sk, m)\big) = sk \oplus (sk \oplus m\ ) = m$$

Perfect security for messages of length n:

For every $m, ct \in \{0,1\}^n$ there exists exactly one sk s.t. $E(sk, m) = ct$.

Therefore, for every $m_0, m_1, ct \in \{0,1\}^n$:

$$\Pr_{sk \leftarrow G(1^n)}[E(sk, m_0) = ct] \ = \ \Pr_{sk \leftarrow G(1^n)}[E(sk, m_1) = ct] = 2^{-n}$$

Therefore, $E(sk, m_0) \equiv E(sk, m_1)$

Theorem [Shannon]: There is no perfectly secure cipher for messages of length $\ell > n$.

Proof: Let (G, E, D) be perfectly secure. Assume for simplicity that E is deterministic.

Fix some ciphertext ct^* in the support of E. By perfect security, for every $m \in \{0,1\}^\ell$:

$$\Pr_{sk \leftarrow G(1^n)}[E(sk, m) = ct^*] > 0.$$

Therefore, for every $m \in \{0,1\}^\ell$ there exists sk_m such that $ct^* = E(sk_m, m)$.

By correctness, for every $m \neq m' \Rightarrow sk_m \neq sk_{m'}$ and therefore there must be at least $2^\ell > 2^n$ keys.

Symmetric Encryption

Theorem: Computationally secure ciphers for $\ell > n$ exist iff one-way functions exist.

Proof: (OWF ⇒ cipher):

Let $G: \{0,1\}^n \to \{0,1\}^{\ell(n)}$ be a PRG:

$$sk \leftarrow \{0,1\}^n, \qquad E(sk, m) = G(sk) \oplus m, \qquad D(sk, c) = G(sk) \oplus c.$$

For every $n \in \mathbb{N}$ and $m_0, m_1 \in \{0,1\}^\ell$ we have $E(sk, m_0) \approx_c E(sk, m_1)$ since:

$$E(sk, m_b) \equiv G(sk) \oplus m_b \approx_c U_\ell \oplus m_b \equiv U_\ell.$$

Q: Can we encrypt twice with the same key?

Multi-Message Security - Known Plaintext Attack

Definition: A cipher (G, E, D) is KPA-secure for $t = t(n)$ messages of length $\ell = \ell(n)$:

$$\left\{\left(E(sk, \vec{m}_0[i])\right)_{1\le i\le t}\right\}_{\substack{n\in\mathbb{N} \\ \vec{m}_0,\vec{m}_1\in\{0,1\}^\ell}} \approx_c \left\{\left(E(sk, \vec{m}_1[i])\right)_{1\le i\le t}\right\}_{\substack{n\in\mathbb{N} \\ \vec{m}_0,\vec{m}_1\in\{0,1\}^\ell}}$$

where $sk \leftarrow G(1^n)$.

We say that (G, E, D) is KPA-secure if it is KPA-secure for every polynomials t, ℓ.

Note: Security is only guaranteed for message that are fixed upfront.

Multi-Message Security - Chosen Plaintext Attack

Definition: A cipher (G, E, D) is CPA-secure if for every poly-size adversary A there exists a negligible function ϵ such that for every $n \in \mathbb{N}$:

$$\Pr_{sk \leftarrow g(1^n),\, b \leftarrow \{0,1\}} \left[A^{O_{sk}^b(\cdot)}(1^n) = b \right] \leq \frac{1}{2} + \epsilon$$

where O_{sk}^b is a (possibly randomized) oracle that given a pair of massages (m_0, m_1) of the same length, returns $E(sk, m_b)$.

Claim: Every CPA-secure cipher is also KPA-secure.

Claim: Assuming OWFs there exists a KPA-secure cipher that is not CPA-secure.

Multi-Message Security

Theorem: KPA-secure ciphers exist iff one-way functions exist.

Proof: (OWF ⇒ cipher):

Given a PRF $F: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ we construct a cipher (G, E, D) as follows:

$E(k \in \{0,1\}^n, m \in \{0,1\})$:

- Sample $r \leftarrow \{0,1\}^n$
- Output $(r, F(k,r) \oplus m)$

Note: No deterministic encryption can be KPA-secure.

Proof sketch: Consider an **ideal** cipher $\left(\tilde{E}, \tilde{D}\right)$ that, instead of a key, access a shared random function $R: \{0,1\}^n \to \{0,1\}$.

We can show that:

$$\left\{\left(\tilde{E}^R(\vec{m}_0[i])\right)_{1\le i\le t}\right\}_{\substack{n\in\mathbb{N}\\ \vec{m}_0,\vec{m}_1\in\{0,1\}}} \approx_s \left\{\left(\tilde{E}^R(\vec{m}_1[i])\right)_{1\le i\le t}\right\}_{\substack{n\in\mathbb{N}\\ \vec{m}_0,\vec{m}_1\in\{0,1\}}}$$

Let $sk \leftarrow \{0,1\}^n$. By PRF security for every $b \in \{0,1\}$:

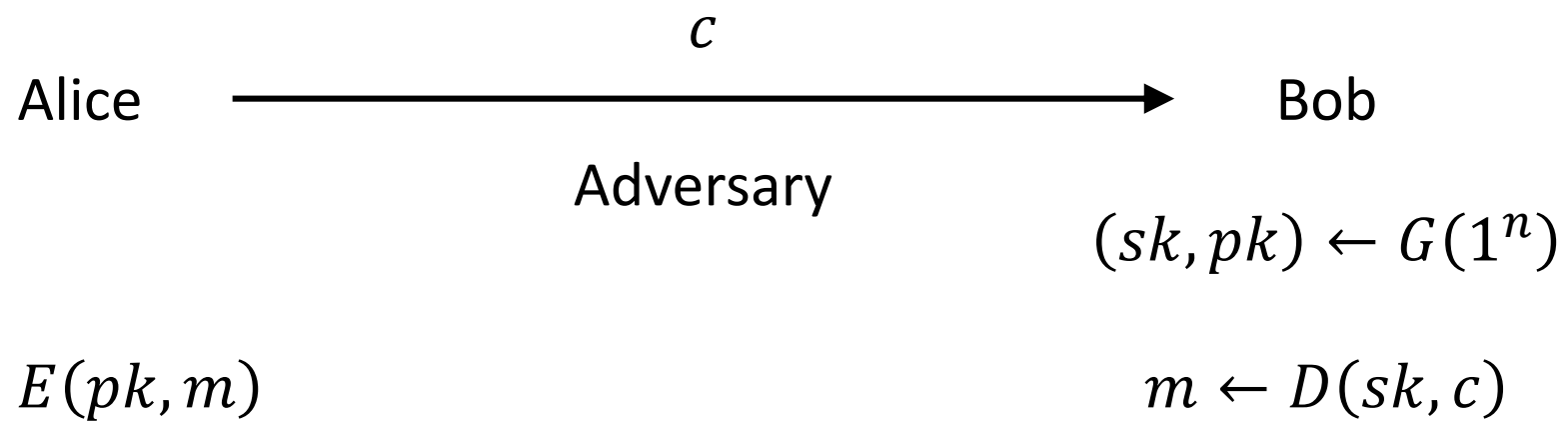
$$\left\{\left(\tilde{E}^{F(sk,\cdot)}(\vec{m}_b[i])\right)_{1\le i\le t}\right\}_{\substack{n\in\mathbb{N}\\ \vec{m}_0,\vec{m}_1\in\{0,1\}}} \approx_c \left\{\left(\tilde{E}^R(\vec{m}_b[i])\right)_{1\le i\le t}\right\}_{\substack{n\in\mathbb{N}\\ \vec{m}_0,\vec{m}_1\in\{0,1\}}}$$

Since $E(sk,m) \equiv \tilde{E}^{F(sk,\cdot)}(m)$, we have:

$$\left\{\left(E(sk,\vec{m}_0[i])\right)_{1\le i\le t}\right\}_{\substack{n\in\mathbb{N}\\ \vec{m}_0,\vec{m}_1\in\{0,1\}}} \approx_c \left\{\left(E(sk,\vec{m}_1[i])\right)_{1\le i\le t}\right\}_{\substack{n\in\mathbb{N}\\ \vec{m}_0,\vec{m}_1\in\{0,1\}}}$$

Public-Key Encryption (PKE)

Bob's public encryption key: pk



Public-Key Encryption (PKE)

Definition: A public-key encryption scheme (G, E, D) is secure against chosen plaintext attack (CPA) if for every poly-size A_1, A_2 there exists a negligible function ϵ such that for every $n \in \mathbb{N}$:

$$\Pr_{\substack{(sk,pk)\leftarrow G(1^n) \\ b\leftarrow\{0,1\}}}\left[\begin{matrix} m_0, m_1 \leftarrow A_1(pk) \\ A_2\big(pk, E(pk, m_b)\big) = b \end{matrix}\right] \leq \frac{1}{2} + \epsilon(n)$$

Notes:

- The adversary can choose m_0, m_1 after seeing pk.
- The definition implies security for many messages.

History

In their 1976 paper “New Directions in Cryptography” Diffie and Helman introduced:

- The notions of public key encryption and digital signatures.
- An abstract template for constructing these objects.
- Their key-exchange protocol.

In 1977 Rivest, Shamir and Adleman developed the first public key encryption and digital signatures based on the template of Diffie and Helman.

	Secret key	Public key
Encryption	**cipher**	**PKE**
	OWF	Discrete Log Factoring/RSA LPN/LWE
Authentication	**MAC**	**Digital signatures**
	OWF	OWF

PKE from Code Obfuscation

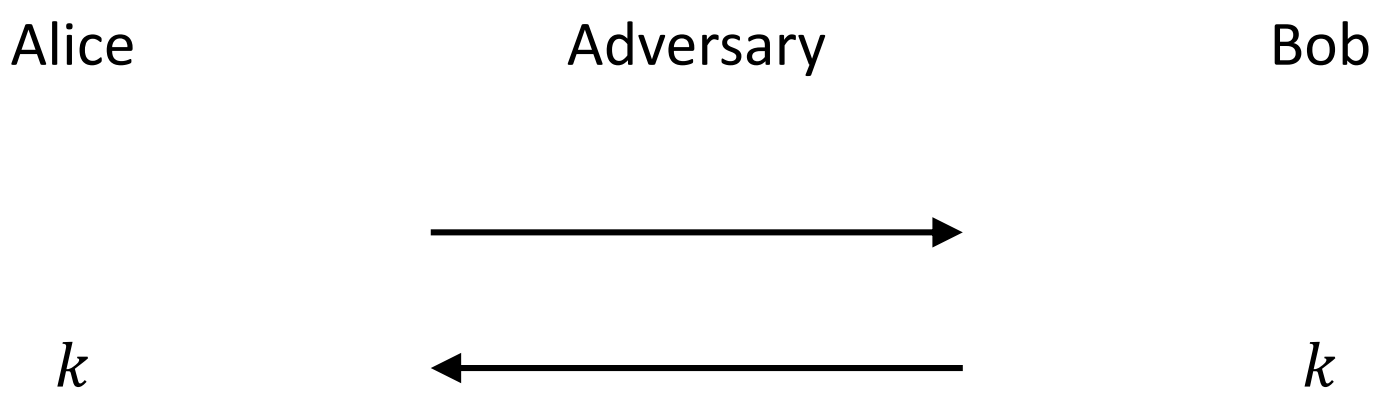
Let (E, D) be a symmetric cipher. We construct a PKE:

$G(1^n)$:

- Sample $k \leftarrow \{0,1\}^n$
- Set $sk = k$
- Set pk to be an **obfuscated code** computing the function $E(k,\cdot)$

Intuition: can execute pk to encrypt, but cannot extract sk from pk.

Key-Exchange Protocol

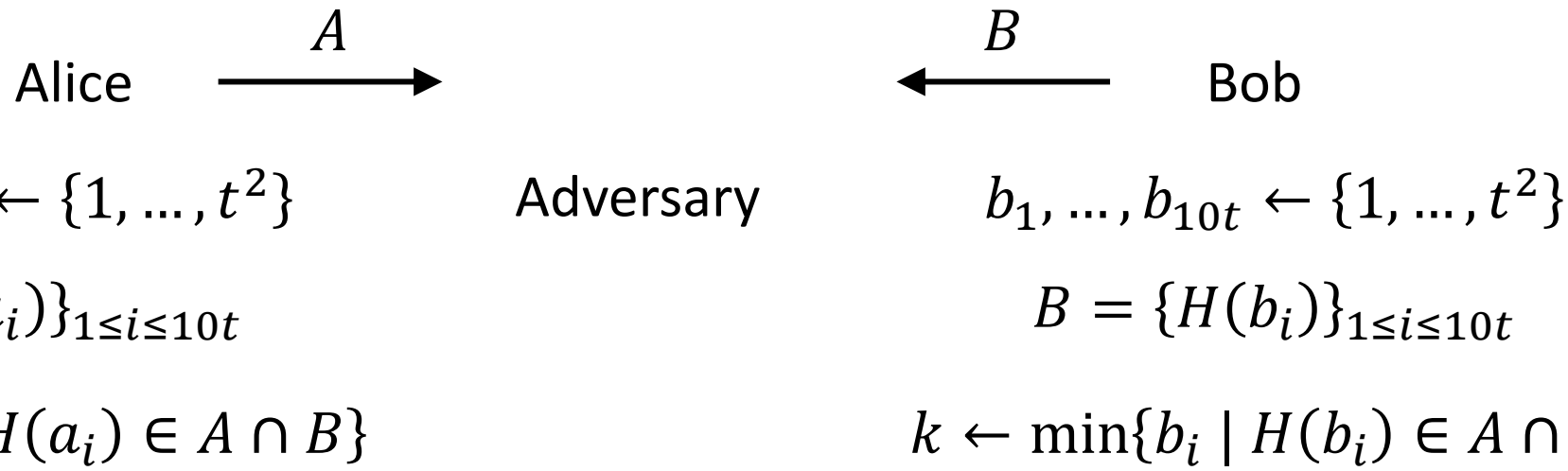


Completeness: Alice and Bob agree on the same key.

Security: The key is pseudorandom even given the messages.

Merkle Key-Exchange

Let $H: \{0,1\}^n \to \{0,1\}^n$ be a hash function. Let t be a parameter ($t \ll 2^{n/2}$).



Completeness: Alice and Bob run in time t and fail to agree with probability $< 2^{-10}$.

Security: assuming H is a random oracle, adversary of size $o(t^2)$ learns nothing.

Beyond Merkle Key-Exchange

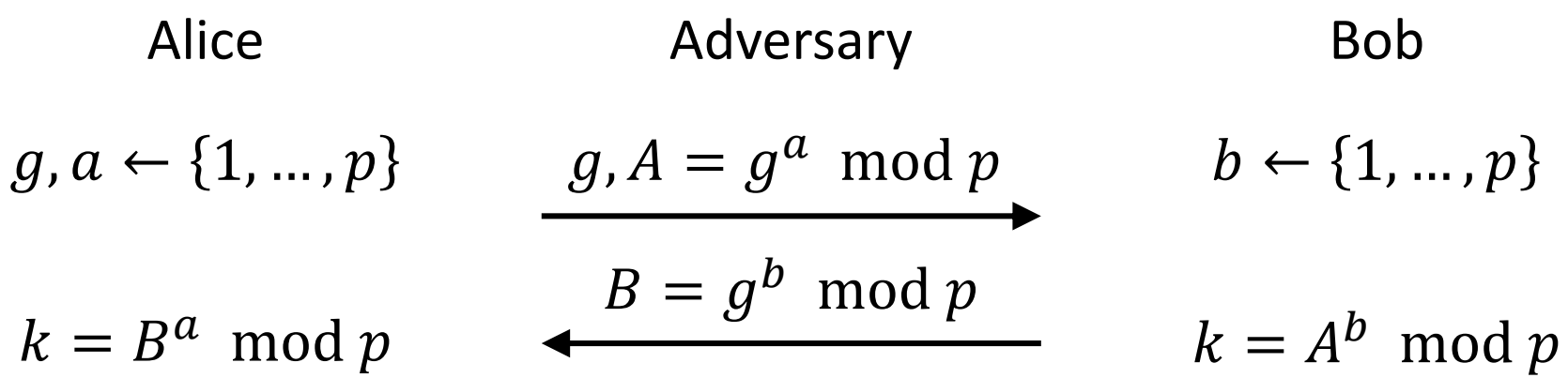
Merkle's protocol gets a quadratic gap between the honest parties and the adversary.

Goal: Key exchange protocol with larger gap (e.g. exponential).

Barrier: Using a PRG\PRF\Hash as a black-box is insufficient.

Solution: Use hard problems from algebra.

Diffie-Helman Key-Exchange Protocol



- Given g, g^a for random g, a, we assume it is hard to find the discrete log a.
- Moreover, given g, g^a, g^b for random g, a, b, we assume it is hard to find g^{ab}.
- While g^{ab} is not pseudorandom given g, g^a, g^b, in some groups we believe it is.

ElGamal PKE

$G(1^n)$:

- Sample an n-bit prime p and $g, a \leftarrow \{1, \dots, p\}$
- Output $\left(sk = (p, a),\ pk = (p, g, A = g^a)\right)$

$E\left((p, g, A), m \in \{0,1\}\right)$:

- Sample $b \leftarrow \{1, \dots, p\}$ and $r \leftarrow \{0,1\}^n$
- Output $\left(r,\ B = g^b,\ \langle A^b, r\rangle \oplus m\ \right)$

$D\left((p, a), (r, B, c)\right)$: Output $\langle B^a, r\rangle \oplus c$

Trapdoor Function (TDF)

Syntax:

- PPT key generator G that given 1^n samples key pair (sk, pk)
- Deterministic poly-time F that given pk and $x \in \{0,1\}^n$ outputs $y \in \{0,1\}^*$
- Deterministic poly-time F^{-1} that given sk and $y \in \{0,1\}^*$ outputs $x \in \{0,1\}^n$

Correctness: for every $x \in \{0,1\}^n$ $\Pr_{(sk,pk)\leftarrow G(1^n)}\left[F^{-1}\left(sk, F(pk,x)\right) = x\right] = 1$

Definition: A TDF (G, F, F^{-1}) is one-way if for every poly-size A there exists a negligible function ϵ such that for all $n \in \mathbb{N}$:

$$\Pr_{\substack{(sk,pk)\leftarrow G(1^n)\\ x\leftarrow\{0,1\}^n}}\left[A_n\left(pk, F(pk,x)\right) = x\right] \leq \epsilon(n)$$

The Diffie-Helman Template

Let (G, F, F^{-1}) be a trapdoor permutation over $\{0,1\}^n$.

- PKE: $E(pk, m) = F(pk, m)$
- Digital signature: $S(sk, m) = F^{-1}(sk, m)$

Clearly insecure by our definitions!

This template is used in practice:

- PKE: $E(pk, m) = F\big(pk, P(m, U_n)\big)$ where P is a random invertible function.
- Digital signature: $S(sk, m) = F^{-1}(sk, H(m))$ where H is a random hash.

KPA-Secure PKE from TDF

Theorem: If TDFs exist then PKE exists.

Proof outline:

Let (G, F, F^{-1}) be a TDF. We construct a PKE (G, E, D):

$E(pk, m \in \{0,1\})$:

- Sample $x, r \leftarrow \{0,1\}^n$
- Output $(F(pk, x),\ r,\ \langle x, r \rangle \oplus m)$

By Goldreich-Levin, $\{pk, E(pk, 0)\} \approx_c \{pk, E(pk, 1)\}$.

The RSA Trapdoor Permutation

- Let p, q be random n-bit primes and let $N = p \cdot q$.
- Let $\mathbb{Z}_N^*$ be the set of integers in $\{1, \ldots, N\}$ that are co-prime to N.
- $|\mathbb{Z}_N^*| = \phi(N) = (p-1)(q-1)$.
- Given N computing $\phi(N)$ is as hard as factoring N.
- Euler's theorem: for every $x \in \mathbb{Z}_N^*$, $x^{\phi(N)} \equiv 1 \bmod N$.
- If e, d are such that $e \cdot d \equiv 1 \bmod \phi(N)$ then for any $x \in \mathbb{Z}_N^*$, $(x^e)^d \equiv x \bmod N$.
- Given N, x, i we can efficiently compute $x^i \bmod N$.
- The RSA assumption asserts that the following is a TDP:

$$F\big((N,e),x\big) = x^e \bmod N, \qquad F^{-1}\big((N,d),y\big) = y^d \bmod N$$

Learning Parity with Noise (LPN)

For $m = 2n$ and $\delta = \frac{1}{2\sqrt{n}}$ let:

- A be a random matrix in $\{0,1\}^{m \times n}$
- s be a random vector in $\{0,1\}^{n}$
- e be a noise vector in $\{0,1\}^{m}$ where every coordinate is 1 with probability δ
- u be a random vector in $\{0,1\}^{m}$

The LPN assumption with parameters m, δ asserts that:

$$\{A, As + e\} \approx_c \{A, u\}$$

PKE from LPN

$G(1^n)$:

- Sample A, s, e as in the LPN problem
- Output $\left(sk = e,\ pk = (A, As + e)\right)$

$E(A', m \in \{0,1\})$:

- If $m = 1$: output a random $v \leftarrow \{0,1\}^m$
- If $m = 0$:
  - Sample a random $y \in \{0,1\}^m$ such that $y^T A' = 0$
  - Sample e' from the same distribution as e
  - Output $y + e'$

$D(e, c)$: output $\langle c, e \rangle$

PKE from LPN

Correctness:

A random encryption of 1 decrypts correctly with probability $\approx \frac{1}{2}$.

Let $y + e'$ be a random encryption of 0. Since $y^T(A, As + e) = 0$ we have that:

$$\langle y + e', e\rangle = \langle y, e\rangle + \langle e', e\rangle = \langle y, As + e\rangle - \langle y, As\rangle + \langle e', e\rangle = \langle e', e\rangle$$

Therefore, since every coordinate of e and e' is 1 with probability $\frac{1}{2\sqrt{n}}$, a random encryption of 0 decrypts correctly with probability $\geq \frac{3}{4}$.

By encrypting each bit n time we can decrypt with negligible error.

PKE from LPN

Security:

It is sufficient to prove security for one bit.

By LPN:

$$\{pk, E(0)\} \equiv \{(A, As + e), y + e'\} \approx_c \{(A, u), y + e'\}$$

$$\{pk, E(1)\} \equiv \{(A, As + e), v\} \approx_c \{(A, u), v\}$$

Let $B \in \{0,1\}^{m \times n'}$ be a random basis for the kernel of (A, u) and let $r \leftarrow \{0,1\}^{n'}$.

Since (A, u) is uniform, so is B.

Therefore, by LPN:

$$\{B, y + e'\} \equiv \{B, Br + e'\} \approx_c \{B, v\} \quad \Rightarrow \quad \{(A, u), y + e'\} \approx_c \{(A, u), v\}$$

Barrier for Basing PKE on OWF

A construction (G, E, D) of PKE from OWF is a **black-box** if:

- For any F, (G^F, E^F, D^F) satisfies correctness.
- There exists PPT B s.t. for any A, F, if A^F breaks (G^F, E^F, D^F) then $B^{A,F}$ inverts F.

Theorem([IR95]): There is no black-box construction of PKE from OWF.

Proof idea: Show that for any (G, E, D) there exists A such that for any F, A^F breaks (G^F, E^F, D^F). A is unbounded but makes only a polynomial number of queries to F.

Assume there is a black-box PKE construction. Therefore there exists B, such that for any F, $B^{A,F}$ inverts F. However, if F is a completely random function it cannot be inverted with polynomial number of queries.